



Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at <http://about.jstor.org/participate-jstor/individuals/early-journal-content>.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

THE AMERICAN MATHEMATICAL MONTHLY.

Entered at the Post-office at Springfield, Missouri, as second-class matter.

VOL. IX.

NOVEMBER, 1902.

No. 11.

A MATRIX DEFINED BY THE QUATERNION GROUP.

By DR. L. E. DICKSON.

1. The Quaternion Group was chosen by Weber* to illustrate his exposition of a portion of Frobenius's theory of group-matrices and group-determinants.† In his treatment of the illustrative example, Weber gives no clue to the reader how his results were obtained originally and makes the verification depend upon two laborious compositions of matrices of order eight. The example may, however, be treated very simply by a method which emphasizes certain remarkable properties enjoyed by group-matrices.

A second purpose of this paper is to furnish an instructive example of the theory of group-matrices as generalized for an arbitrary field (Körper, realm of rationality) by the writer.‡ The canonical forms are essentially different in the cases of a field having modulus 2 and a field not having modulus 2. The methods used are elementary and the paper is entirely independent of those cited. Incidentally, it illustrates a method of factoring important determinants.

2. The Quaternion Group may be defined by the multiplication-table§

*Weber, *Algebra*, edition of 1899, vol. 2, pp. 216-218; pp. 125-128.

†For an elementary, but complete, exposition of Frobenius's theory, see the writer's article in the *Annals of Mathematics*, October, 1902.

‡Dickson, *Transactions American Mathematical Society*, vol. 3 (1902), pp. 285-301; further developments in *University of Chicago Decennial Publications*, vol. IX, pp. 35-51.

§The arrangement of the multipliers in the first column is such that the products equal to the identity element x_1 all appear in the main diagonal.

	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
x_1	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
x_2	x_2	x_1	x_4	x_3	x_6	x_5	x_8	x_7
x_4	x_4	x_3	x_1	x_2	x_7	x_8	x_6	x_5
x_3	x_3	x_4	x_2	x_1	x_8	x_7	x_5	x_6
x_6	x_6	x_5	x_8	x_7	x_1	x_2	x_3	x_4
x_5	x_5	x_6	x_7	x_8	x_2	x_1	x_4	x_3
x_8	x_8	x_7	x_5	x_6	x_4	x_3	x_1	x_2
x_7	x_7	x_8	x_6	x_5	x_3	x_4	x_2	x_1

The body of this table is a matrix M of order eight called the *group-matrix* of the Quaternion Group. Consider a transformation T on eight variables $\xi_1, \dots, \xi_8$ whose coefficients form the matrix M and are elements of a given field F .

3. Suppose first that the field F does not have modulus 2, so that division by 2 is possible in the field. An inspection of matrix M leads to certain linear functions which transformation T multiplies by constants:

$$\begin{aligned}\eta_1 &= \xi_1 + \xi_2 + \xi_3 + \xi_4 + \xi_5 + \xi_6 + \xi_7 + \xi_8, & \eta_3 &= \xi_1 + \xi_2 - \xi_3 - \xi_4 + \xi_5 + \xi_6 - \xi_7 - \xi_8, \\ \eta_2 &= \xi_1 + \xi_2 + \xi_3 + \xi_4 - \xi_5 - \xi_6 - \xi_7 - \xi_8, & \eta_4 &= \xi_1 + \xi_2 - \xi_3 - \xi_4 - \xi_5 - \xi_6 + \xi_7 + \xi_8.\end{aligned}$$

Indeed, T replaces them by the respective functions

$$(1) \quad \eta_1' = \sigma_1 \eta_1, \quad \eta_2' = \sigma_2 \eta_2, \quad \eta_3' = \sigma_3 \eta_3, \quad \eta_4' = \sigma_4 \eta_4,$$

where the following abbreviations have been used:

$$\begin{aligned}\sigma_1 &= x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8, & \sigma_3 &= x_1 + x_2 - x_3 - x_4 + x_5 + x_6 - x_7 - x_8, \\ \sigma_2 &= x_1 + x_2 + x_3 + x_4 - x_5 - x_6 - x_7 - x_8, & \sigma_4 &= x_1 + x_2 - x_3 - x_4 - x_5 - x_6 + x_7 + x_8.\end{aligned}$$

From the definitions of $\eta_1, \eta_2, \eta_3, \eta_4$, we get

$$\begin{aligned}\xi_1 + \xi_2 &= \frac{1}{4}(\eta_1 + \eta_2 + \eta_3 + \eta_4), & \xi_5 + \xi_6 &= \frac{1}{4}(\eta_1 - \eta_2 + \eta_3 - \eta_4), \\ \xi_3 + \xi_4 &= \frac{1}{4}(\eta_1 + \eta_2 - \eta_3 - \eta_4), & \xi_7 + \xi_8 &= \frac{1}{4}(\eta_1 - \eta_2 - \eta_3 + \eta_4).\end{aligned}$$

Hence $\eta_1, \eta_2, \eta_3, \eta_4$ may be introduced as new independent variables in place of four of the original variables. Also, if we set

$$s_1 = \xi_1 - \xi_2, \quad s_2 = \xi_3 - \xi_4, \quad s_3 = \xi_5 - \xi_6, \quad s_4 = \xi_7 - \xi_8,$$

the functions $\eta_1, \eta_2, \eta_3, \eta_4, s_1, s_2, s_3, s_4$ are evidently linearly independent functions of $\xi_1, \dots, \xi_8$ and may be introduced as new variables in place of the latter. Now T replaces s_1, s_2, s_3, s_4 by the respective functions

$$\begin{aligned}
 s_1' &= as_1 + bs_2 + cs_3 + ds_4, \\
 (2) \quad s_2' &= -bs_1 + as_2 + ds_3 - cs_4, \\
 s_3' &= -cs_1 - ds_2 + as_3 + bs_4, \\
 s_4' &= -ds_1 + cs_2 - bs_3 + as_4,
 \end{aligned}$$

where

$$a = x_1 - x_2, \quad b = x_3 - x_4, \quad c = x_5 - x_6, \quad d = x_7 - x_8.$$

It follows as before that $\sigma_1, \sigma_2, \sigma_3, \sigma_4, a, b, c, d$ are linearly independent functions of $x_1, x_2, \dots, x_8$.

Let first the quantity $i \equiv \sqrt{-1}$ belong to the field F and set

$$\eta_5 = s_1 - is_2, \quad \eta_6 = s_3 + is_4, \quad \eta_7 = -s_3 + is_4, \quad \eta_8 = s_1 + is_2,$$

so that $\eta_5, \eta_6, \eta_7, \eta_8$ are linearly independent functions of s_1, s_2, s_3, s_4 . Then the transformation defined by (1) and (2) takes the canonical form

$$(3) \quad \begin{cases} \eta_1' = \sigma_1 \eta_1, & \eta_3' = \sigma_3 \eta_3, & \eta_5' = \kappa \eta_5 + \lambda \eta_6, & \eta_7' = \kappa \eta_7 + \lambda \eta_8, \\ \eta_2' = \sigma_2 \eta_2, & \eta_4' = \sigma_4 \eta_4, & \eta_6' = \mu \eta_5 + \nu \eta_6, & \eta_8' = \mu \eta_7 + \nu \eta_8, \end{cases}$$

where

$$\kappa = a + ib, \quad \lambda = c - id, \quad \mu = -c - id, \quad \nu = a - ib.$$

In particular, the determinant of transformation (3), and hence of matrix M , equals

$$\sigma_1 \sigma_2 \sigma_3 \sigma_4 (\kappa \nu - \lambda \mu)^2 \equiv \sigma_1 \sigma_2 \sigma_3 \sigma_4 (a^2 + b^2 + c^2 + d^2)^2.$$

As a corollary, we derive for the determinant of (2) the known formula

$$\begin{vmatrix} a & b & c & d \\ -b & a & d & -c \\ -c & -d & a & b \\ -d & c & -b & a \end{vmatrix} = (a^2 + b^2 + c^2 + d^2)^2.$$

Suppose next that i does not belong to the field F . Then the transformation T of matrix M of coefficients belonging to F cannot be reduced to the canonical form (3) by means of a transformation of variables with coefficients in F . In fact, $a^2 + b^2 + c^2 + d^2$ cannot be expressed in the form $\kappa \nu - \lambda \mu$, where $\kappa, \lambda, \mu, \nu$ are linear functions of a, b, c, d with coefficients in F (not containing i). As the canonical form of T for the field F , we therefore take the transformation defined by (1) and (2). For the enlarged field $F(i)$, obtained by adjoining i to F , we may take as the canonical form either (3) or, preferably, the transformation

$$(3') \quad \begin{cases} \eta_1' = \sigma_1 \eta_1, & \eta_3' = \sigma_3 \eta_3, & \eta_5' = \frac{\kappa \eta_5 + \lambda \eta_6}{\lambda}, & \eta_7' = \frac{\kappa \eta_7 + \lambda \eta_8}{\lambda}, \\ \eta_2' = \sigma_2 \eta_2, & \eta_4' = \sigma_4 \eta_4, & \eta_6' = -\frac{\kappa \eta_5 + \lambda \eta_6}{\lambda}, & \eta_8' = -\frac{\kappa \eta_7 + \lambda \eta_8}{\lambda}, \end{cases}$$

where $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ are arbitrary quantities in F , while κ, λ are arbitrary quantities in $F(i)$, $\bar{\kappa}$ denoting the conjugate of κ .

4. We may now readily determine the order of the group* of all transformations of matrix M of coefficients in the Galois Field of order p^n , $p > 2$.

Let first i belong to the $GF[p^n]$, so that $p^n - 1$ is a multiple of 4, the period of i . We have then to determine the number of the transformations (3) of determinant not zero. Here $\sigma_1, \sigma_2, \sigma_3, \sigma_4, \kappa, \lambda, \mu, \nu$ are any elements of the $GF[p^n]$ such that

$$(4) \quad \sigma_1 \sigma_2 \sigma_3 \sigma_4 (\kappa \nu - \lambda \mu)^2 \neq 0,$$

so that the order of the group is $(p^n - 1)^4 \cdot (p^{2n} - 1)(p^{2n} - p^n)$.

Let next i be not in the $GF[p^n]$, so that it serves to extend the $GF[p^n]$ to the $GF[p^{2n}]$. We have then to determine the number of transformations (3') of the determinant not zero. Here $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ are any elements $\neq 0$ of the $GF[p^n]$, while κ and λ are any elements of the $GF[p^n]$ such that

$$\Delta \equiv \kappa \bar{\kappa} + \lambda \bar{\lambda} \equiv \kappa^{p^n+1} + \lambda^{p^n+1} \neq 0.$$

But $\Delta = 0$ gives $\kappa = \tau \lambda$, where $\tau^{p^n+1} = -1$. Hence there are

$$1 + (p^{2n} - 1)(p^n + 1)$$

sets κ, λ making $\Delta = 0$. Subtracting this sum from p^{4n} , the total number of sets κ, λ in the $GF[p^{2n}]$, we obtain $(p^{2n} - 1)(p^{2n} - p^n)$ as the number of sets κ, λ making $\Delta \neq 0$. Hence the order is again†

$$(p^n - 1)^4 \cdot (p^{2n} - 1)(p^{2n} - p^n).$$

5. Suppose finally that the field F has modulus 2. The four functions in §3 which T multiplies by constants are now identical. We seek eight linear functions $\eta_1, \dots, \eta_8$ which are linearly independent function modulo 2 of

*In view of the canonical form (3) or (3'), the totality of the transformations T evidently possesses the group property.

†Another method, not assuming the independence of $\sigma_1, \sigma_2, \sigma_3, \sigma_4, \kappa, \lambda, \mu, \nu$, consists in finding the number of sets $x_1, \dots, x_8$ for which

$$\begin{array}{l|l} \sigma_1 \neq 0, \sigma_2 \neq 0, \sigma_3 \neq 0, \sigma_4 \neq 0, \kappa \nu - \lambda \mu = 0 & p^n(p^{2n} + p^n - 1)(p^n - 1)^4 \\ \sigma_1 \neq 0, \sigma_2 \neq 0, \sigma_3 \neq 0, \sigma_4 = 0 & p^{4n}(p^n - 1)^3 \\ \sigma_1 \neq 0, \sigma_2 \neq 0, \sigma_3 = 0 & p^{5n}(p^n - 1)^2 \\ \sigma_1 \neq 0, \sigma_2 = 0 & p^{6n}(p^n - 1) \\ \sigma_1 = 0 & p^{7n} \end{array}$$

Subtracting the sum of the numbers in the last column from p^{8n} , the total number of sets $x_1, \dots, x_8$, we obtain $p^n(p^n + 1)(p^n - 1)^6$ as the number of sets $x_1, \dots, x_8$ for which (4) holds, and hence equals the order of the group.

$\xi_1, \dots, \xi_8$ such that T replaces each η_i by a linear function of $\eta_1, \dots, \eta_i$. The desired functions are

$$\begin{aligned}\eta_1 &= \xi_1 + \xi_2 + \xi_3 + \xi_4 + \xi_5 + \xi_6 + \xi_7 + \xi_8, & \eta_2 &= \xi_1 + \xi_2 + \xi_3 + \xi_4, \\ \eta_3 &= \xi_1 + \xi_2 + \xi_7 + \xi_8, & \eta_4 &= \xi_1 + \xi_2, & \eta_5 &= \xi_1 + \xi_3 + \xi_5 + \xi_7, \\ \eta_6 &= \xi_1 + \xi_3, & \eta_7 &= \xi_1 + \xi_5, & \eta_8 &= \xi_1.\end{aligned}$$

To prove them linearly independent modulo 2, we note that linear combinations of $\eta_1, \eta_2, \eta_3, \eta_4$ give $\xi_1 + \xi_2, \xi_3 + \xi_4, \xi_5 + \xi_6, \xi_7 + \xi_8$; while linear combinations of $\eta_5, \eta_6, \eta_7, \eta_8$ give $\xi_1, \xi_3, \xi_5, \xi_7$. We find that T gives rise to the following transformation:

$$\begin{aligned}\eta_1' &= \rho_1 \eta_1, \\ \eta_2' &= \rho_2 \eta_1 + \rho_1 \eta_2, \\ \eta_3' &= \rho_3 \eta_1 + \rho_1 \eta_3, \\ \eta_4' &= \rho_4 \eta_1 + \rho_3 \eta_2 + \rho_2 \eta_3 + \rho_1 \eta_4, \\ \eta_5' &= \rho_5 \eta_1 + (\rho_2 + \rho_3) \eta_2 + \rho_3 \eta_3 + \rho_1 \eta_5, \\ \eta_6' &= \rho_6 \eta_1 + (\rho_3 + \rho_4 + \rho_5) \eta_2 + \rho_4 \eta_3 + \rho_3 \eta_4 + \rho_1 \eta_6, \\ \eta_7' &= \rho_7 \eta_1 + (\rho_2 + \rho_3 + \rho_5) \eta_2 + (\rho_3 + \rho_4 + \rho_5) \eta_3 + \rho_2 \eta_4 + (\rho_2 + \rho_3) \eta_5 + \rho_1 \eta_7, \\ \eta_8' &= \rho_8 \eta_1 + (\rho_3 + \rho_4 + \rho_5 + \rho_6 + \rho_7) \eta_2 + \rho_6 \eta_3 + (\rho_3 + \rho_4 + \rho_5) \eta_4 + (\rho_2 + \rho_4) \eta_5 + (\rho_2 + \rho_3) \eta_6 + \rho_2 \eta_7 + \rho_1 \eta_8,\end{aligned}$$

the coefficients having the following values:

$$\begin{aligned}\rho_1 &= x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8, & \rho_2 &= x_5 + x_6 + x_7 + x_8, \\ \rho_3 &= x_3 + x_4 + x_5 + x_6, & \rho_4 &= x_5 + x_6, & \rho_5 &= x_2 + x_3 + x_6 + x_8, \\ \rho_6 &= x_6 + x_8, & \rho_7 &= x_2 + x_6, & \rho_8 &= x_6.\end{aligned}$$

The determinant of the transformation is evidently ρ_1^8 . The only condition on $\rho_1, \dots, \rho_8$ is, therefore, that $\rho_1 \not\equiv 0$. Hence the order of the group in the $GF[2^n]$ is $2^{7n}(2^n - 1)$.

Since the expressions for $\eta_1', \eta_2', \eta_3', \eta_4'$ remain unaltered by the interchange of the variables η_i with the parameters ρ_i , we have a four-parameter commutative subgroup on the variables $\eta_1, \eta_2, \eta_3, \eta_4$.

A five-parameter commutative subgroup is obtained by setting $x_3 = x_4, x_5 = x_6, x_7 = x_8$, so that $\rho_2 = \rho_3 = \rho_4 \equiv 0 \pmod{2}$. Also

$$\rho_1 = x_1 + x_2, \quad \rho_5 = x_2 + x_3 + x_6 + x_8, \quad \rho_6 = x_6 + x_8, \quad \rho_7 = x_2 + x_6, \quad \rho_8 = x_6$$

are linearly independent functions of x_1, x_2, x_3, x_6, x_8 modulo 2. The above transformation now becomes

$$\begin{aligned}
\eta_1' &= \rho_1 \eta_1, & \eta_5' &= \rho_1 \eta_5 + \rho_5 \eta_1, \\
\eta_2' &= \rho_1 \eta_2, & \eta_6' &= \rho_1 \eta_6 + \rho_6 \eta_1 & + \rho_5 \eta_2, \\
\eta_3' &= \rho_1 \eta_3, & \eta_7' &= \rho_1 \eta_7 + \rho_7 \eta_1 & + \rho_5 \eta_2 + \rho_5 \eta_3, \\
\eta_4' &= \rho_1 \eta_4, & \eta_8' &= \rho_1 \eta_8 + \rho_8 \eta_1 + (\rho_5 + \rho_6 + \rho_7) \eta_2 + \rho_6 \eta_3 + \rho_5 \eta_4.
\end{aligned}$$

Denoting this transformation by T_ρ , we verify that $T_\rho T_\rho = T_{\rho^2}$, where

$$\begin{aligned}
\rho_1'' &= \rho_1 \rho_1', & \rho_5'' &= \rho_5 \rho_1' + \rho_1 \rho_5', & \rho_6'' &= \rho_6 \rho_1' + \rho_1 \rho_6', \\
\rho_7'' &= \rho_7 \rho_1' + \rho_1 \rho_7', & \rho_8'' &= \rho_8 \rho_1' + \rho_1 \rho_8'.
\end{aligned}$$

Hence the transformations T_ρ form a group and the group is commutative. As this result is in accord with the general theory, we have a complete check upon the above work.

The University of Chicago, October 10, 1902.

THE LENGTH OF THE CIRCLE.

By DR. GEORGE BRUCE HALSTED.

The simple theorem of Euclid (Eu. I. 20) that any two sides of a triangle are together greater than the third, appears in popular geometries as a result, a deduction from the definition: the straight line is the shortest distance between two points. But such a definition is, as Hilbert says, *senseless* if one has not defined the concept length.

Without presupposing the idea of the length of the curve, it cannot use anything but the straight, and so is merely a *petitio principii*.

In fact, as Hilbert points out, the essential content of the statement, the straight line is the shortest distance between two points, reduces merely to this theorem of Euclid.

The same fallacy lurks in the theorem, "An arc of a circle is less than any line which envelops it and has the same extremities," recently 'borrowed' by Wentworth (1899, p. 219, Book V, Proposition VII, §451) from Chauvenet (1869, 1881, p. 155, Book V, Proposition XII, §32). He says "Of all the lines, etc., there must be at least one shortest line."

But what is the length of a curve? Again we have a begging of the question. Upon these two holes, empty places, or chasms, he then attempts to rest a demonstration that the length of a circle is the limit of the lengths of the perimeters of inscribed polygons.

The sooner this procedure is banished from elementary geometry the better for the world.

Fortunately there is here no need to touch that very difficult general question, what is the length of a curve in general.

We have only for consideration the simplest of curves, the circle.